

# FortiGate Connector for the HPE VAN SDN - Administration Guide

Version 1.1

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

**FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

**FORTIGUARD CENTER**

<http://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



Tuesday, May 24, 2016

FortiConnector for HPE VAN SDN Controller v.1.1- Administration Guide

# TABLE OF CONTENTS

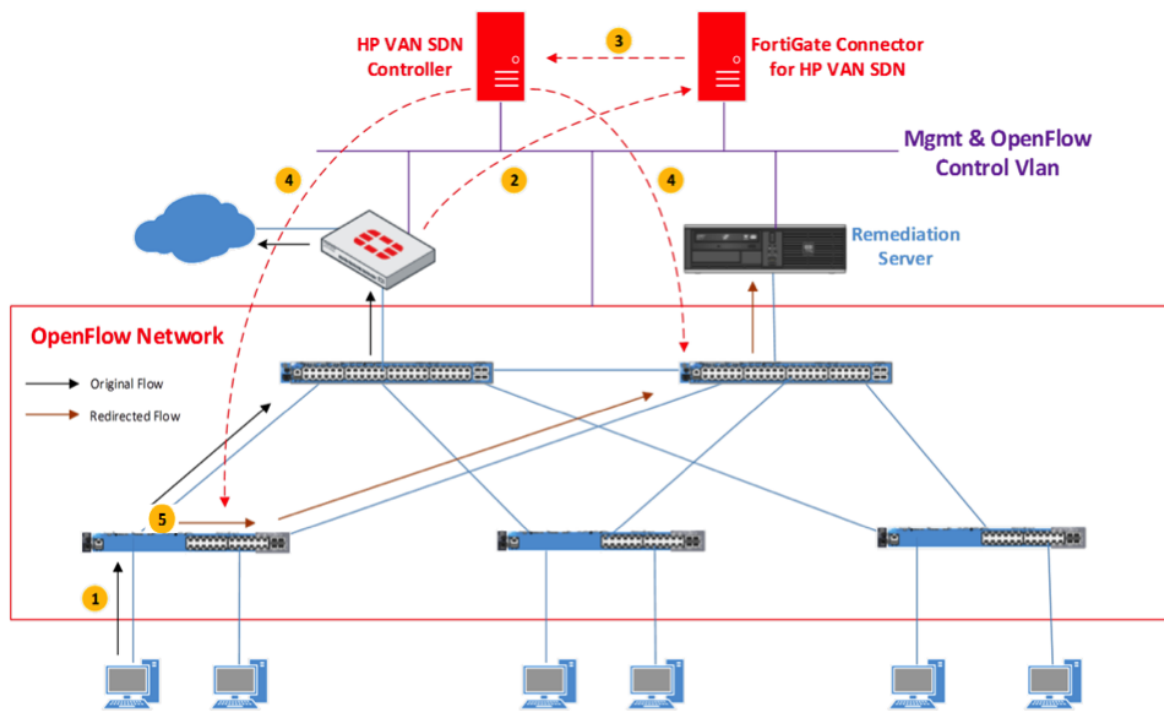
<b>Change Log</b>	<b>4</b>
<b>Overview</b>	<b>5</b>
Licensing	6
Supported Products	6
FortiGate products	6
HP products	6
Features	6
Prerequisites	6
<b>Installation</b>	<b>8</b>
Change Default root password	8
Change default IP address	9
Change system time	9
Change default GUI management credential	9
Login Page	10
Configuration Page	10
Authentication verification and connectivity discovery	11
Starting the FortiGate Connector	13
Stopping the FortiGate Connector	14
Clear the configuration and stop FortiGate Connector	14
<b>Supported use scenarios</b>	<b>16</b>
Prevention scenarios	16
Remediation scenarios	16
<b>Basic Troubleshooting</b>	<b>17</b>
Verify flow pushed by FortiGate Connector on HP SDN Controller for prevention	17
Verify flow pushed by FortiGate Connector on HP switch for prevention	18
Verify flow pushed by FortiGate Connector on HP SDN Controller for remediation	19
Verify flow pushed by FortiGate Connector on HP switch for remediation	19

## Change Log

Date	Change Description
2016-05-13	Initial Release of v.1.1

# Overview

FortiGate Connector for HPE VAN SDN is the Fortinet solution that provides preventive action or remediating action to a problematic endpoint causing security threats to the network. A preventive action isolates an endpoint from the rest of the network in case it generates malicious traffic such that from an exploit or from botnet command and control. The purpose of prevention is to block the user's traffic as close as possible to the connected switch and therefore prevent spread of attack to the rest of the network. A remediating action redirects the traffic of a problematic endpoint to a designated destination that acts as a remediation server. The server provides services to the endpoint such as antivirus database update and software patching. FortiGate Connector is also named as FortiConnector for short in documentation.



## Number key for diagram:

1. Flow detection on FortiGate
2. FortiGate sends sys log message with 5-tuple of flow to FortiGate SDN Connector
3. FortiGate APP sends prevention action for this flow with 5-tuple through RESTful-API
4. Based on flow information and action type received from FortiGate Connector, HPE SDN Controller programs flow in HP OpenFlow switch through OpenFlow protocol with drop or redirection action.
5. Flow is blocked on HP switch port which the infected user is connected to, or redirected to a remediation server

In the products, HPE VAN SDN is also referred as HP VAN SDN, and FortiGate Connector as FortiConnector.

## Licensing

FortiGate Connector for HP VAN SDN is free of charge for Fortinet customers. Your FortiGate must be registered with FortiCare at <https://support.fortinet.com>. Also, you will need to agree with the general Fortinet license agreement. The agreement can be found at <http://www.fortinet.com/doc/legal/EULA.pdf>.

## Supported Products

### FortiGate products

- All physical FortiGate devices running:
  - FortiOS 5.2
  - FortiOS 5.4
- A versions of FortiGate-VM running:
  - FortiOS 5.2
  - FortiOS 5.4

### HP products

- HPE VAN SDN Controller version: 2.6.8
- HP Switch version: X.16.01.0004,
- HP Switch Models supporting prevention action: All switches of OpenFlow capability.
- HP Switch Models supporting remediation action: 2900 series, 3800 series.
- Some models of HP switches have limitation of remediation action. Please see release notes.

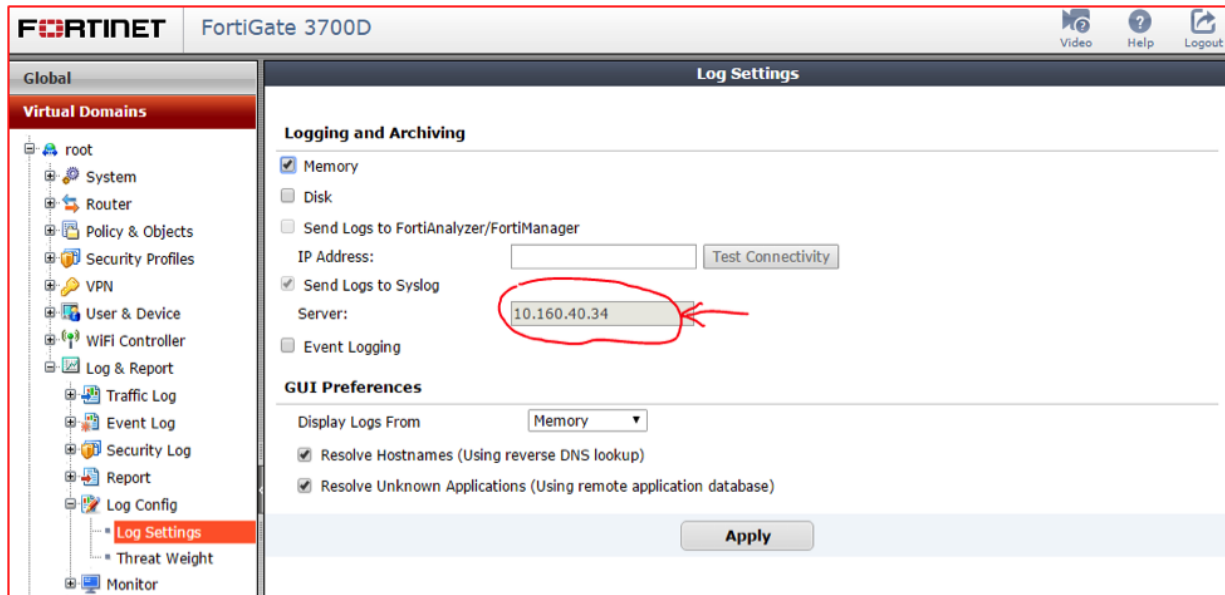
## Features

The FortiGate Connector for HPE VAN SDN version 1.1 supports the following functions:

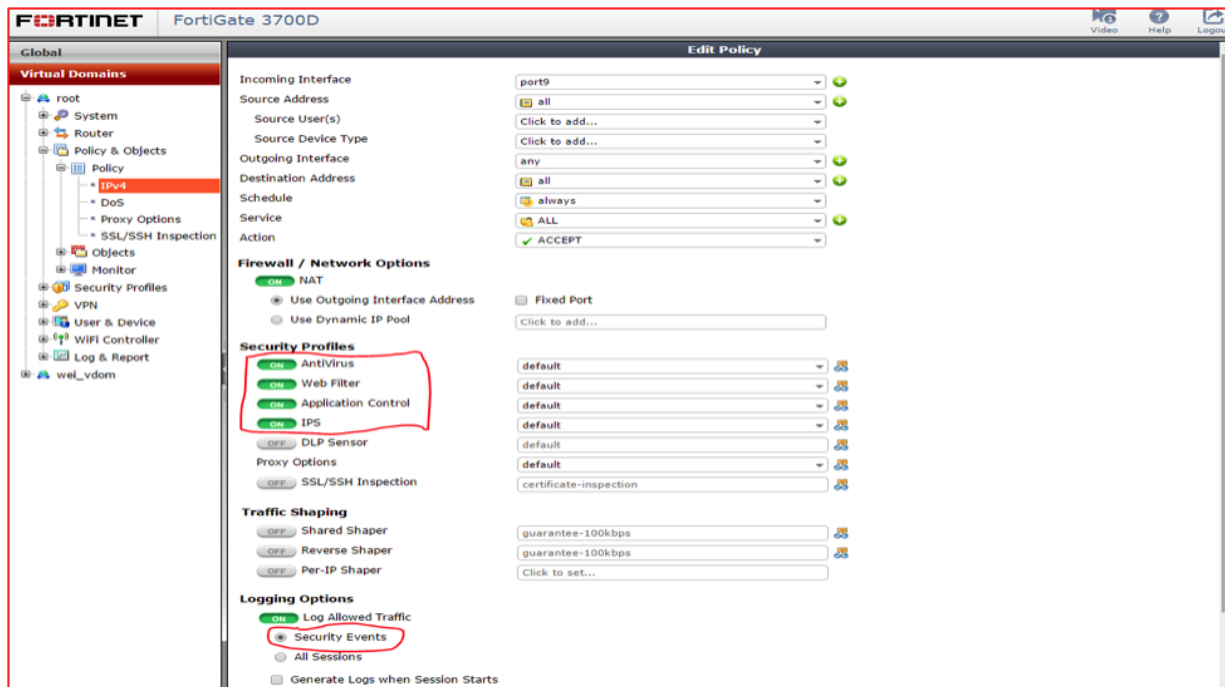
- Prevention or remediation action based on the results of scans by the AntiVirus engine.
- Prevention or remediation action based on the results of scans by the Intrusion Prevention System (IPS) engine.
- Prevention or remediation action based on scans set by parameters in the Application Control Profile.
- Prevention or remediation action based on scans set by parameters in the Web Filter Security Profile.

## Prerequisites

- The FortiGate Connector IP address should be entered in the field for the Syslog server IP address on the FortiGate.



- In order for the FortiGate Connector to make use of the **Security Profiles**, the profiles, as well as the **Security Events** option, need to be enabled on the FortiGate.



# Installation

FortiGate Connector for HPE VAN SDN version 1.1 is packaged in two forms of release:

- Full package in a zip file that contains a VMware OVF release.
- Upgrade package in a zip file for directly upgrading FortiConnector version 1.0 systems to version 1.1.

The full package `FortiConnector-1.1.5-GA.zip` is released for a brand new installation. After the package is unzipped, VMware EXSi 5.5 or 6.0 should be used to install the OVF file with its relating files in the package.

If the upgrade package is going to be installed on the base of FortiConnector 1.0, a third party package must be installed first. The user can log in the console of the FortiConnector and issue the command:

```
sudo apt-get install apache2-utils
```

The upgrade package `FortiConnector-1.1.5-GA-upgrade.zip` can be deployed by the following procedure:

1. On the WEB interface, stop and clear the FortiConnector if it is running.
2. Login to the console of the FortiConnector with the root administrator credential.(default forticonnector/fortinet)
3. Stay in the FortiConnector home directory, install the third party package `apache2-utils` as above.
4. Rename the 'workspace' directory to a backup directory, e.g. type command: `mv workspace workspace-old`
5. FTP or SCP the upgrade package to the FortiConnector home directory.
6. Enter command: `install.sh FortiConnector-1.1.5-GA-upgrade.zip`
7. Refresh the WEB interface page and start using the new FortiConnector version.

## Change Default root password

The default root credentials for FortiGate Connector for HP VAN SDN are:

- User name = `forticonnector`
- Password = `fortinet`

The user name cannot be changed but the password can be changed using the following steps:

1. Use the default root credentials to login to the FortiGate Connector.
2. At the prompt execute the following command:

```
passwd
```

The results will be:

```
Changing password for forticonnector.  
(current) UNIX password:
```

3. Enter the current password which should be the default password `fortinet`.  
Enter new UNIX password:



4. Enter the new password that you want to use.

Retype new UNIX password:

5. Verify the password by retyping it. If all done correctly the result should be:

passwd: password updated successfully

## Change default IP address

The default IP address is 192.168.1. 99

The IP address can be changed using the following command:

```
sudo ifconfig eth0 <new_IP_address> netmask <new_subnet_mask>
```

## Change system time

FortiConnector's system time must be changed to the current time and should match that of the HPE VAN SDN Controller. It is strongly recommended network time protocol (NTP) server be used for time synchronization, by adding desired NTP server to the NTP configuration `/etc/ntp.conf` using an editor:

```
server <ntp_server_name_or_IP>
```

Restart the NTP by the command: `sudo service ntp restart`

## Change default GUI management credential

The default login credentials of the GUI management interface are:

- User name = admin
- Password = admin

The user name and password can be changed using the following steps:

1. Login to the FortiConnector console with user name 'forticonnector' and its password.
2. Use the following command to change the password of the default user 'admin'

```
sudo htpasswd /etc/apache2/.htpasswd admin
```

Enter current password and then enter the new password.

3. If needed, a new user can be added

```
sudo htpasswd /etc/apache2/.htpasswd <new_username>
```

Then assign password to this new user.




It is strongly recommended that the default user admin's password be changed as early as possible.

---

## Login Page

Logging into the GUI management interface is done by using the HTTPS prefix and the device's address in your browser as a URL. The default URL would be `https://192.168.1.99`. If the default IP address is still in use but your computer's address on a different subnet you will need to temporarily change the IP address of your computer to be on the same subnet.

---

 **FortiGate Connector**

Username:

Password:

[LOGIN](#)

---

## Configuration Page

Once on the configuration page of the FortiGate Connector there are some configuration settings that may need to be changed to integrate the device and set the preferences for your network:

- Configure the IP address for the HP VAN SDN Controller, as well as access credentials.
- Configure the IP address for the FortiGate, as well as access credentials.
- Configure the IP address of the Remediation Server if remediation action is going to be selected.
- Configure Action type for each security type: None, Prevention, or Remediation.
- Configure flow timeout value for each security type. Enter 0 for no timeout given to the SDN controller.

HP VAN SDN

Logout

**HP VAN SDN Controller**  
IP Address:   
Username:   
Password:   
Domain:

**FortiGate**  
IP Address:   
Username:   
Password:

**Remediation Server**  
IP Address:

Security Type	Event	SDN Action	Timeout(sec)
AntiVirus	Severe virus detected	<input type="text" value="None"/>	<input type="text" value="600"/>
Application Control	Detected application to be blocked	<input type="text" value="Prevention"/>	<input type="text" value="500"/>
Intrusion Protection	Attack of intrusion detected	<input type="text" value="Remediation"/>	<input type="text" value="65535"/>
Web Filter	Access to blocked URL	<input type="text" value="None"/>	<input type="text" value="600"/>

**Event Logs**  

**Welcome!**  
FortiGate Connector is an application providing SDN security for HP environments. As SDN matures and deployment is considered for enterprise networks, the Fortinet and HP SDN integration enables security scenarios between Fortinet's FortiGate Next Generation Firewall and the HP VAN SDN Controller.

**Status:** clear

## Authentication verification and connectivity discovery

Before starting FortiConnector, a user can click the “Verify” button to verify its authorized connectivity to the HP VAN SDN Controller and the FortiGate respectively. The “Discover” button of Remediation Server will work only if one or more remediation action is turned on, the failure of Remediation server discovery may bring user’s attention to trouble shooting the issue (A recommendation is that the user manually generate traffic from Remediation server to trigger that SDN controller learns Remediation server; user needs to click “Discover” button again to make sure the discover button in green state.). If verification or discovery is successful, the result is displayed in the footnote area under status, and the corresponding Verify/Discover button becomes green color. Otherwise, an error message shows under “Status:” and “Verify” button and “Discover” button are in red state.

When FortiConnector is running, configuration changes of SDN, Fortigate and Remediation server won’t take effect and “Verify” and “Discover” buttons are not function, until the FortiConnector is stopped and run again.

**FortiGate Connector**
HP VAN SDN ▼ Logout

**HP VAN SDN Controller**

IP Address: 10.160.40.32

Username: sdn

Password: ••••••

Domain: sdn

Verify

**FortiGate**

IP Address:

Username:

Password:

Verify

**Remediation Server**

IP Address:

Discover

Security Type	Event	SDN Action	Timeout(sec)
AntiVirus	Severe virus detected	None <span style="border: 1px solid black; padding: 0 5px;">▼</span>	600 <span style="border: 1px solid black; padding: 0 5px;">↕</span>
Application Control	Detected application to be blocked	None <span style="border: 1px solid black; padding: 0 5px;">▼</span>	600 <span style="border: 1px solid black; padding: 0 5px;">↕</span>
Intrusion Protection	Attack of intrusion detected	None <span style="border: 1px solid black; padding: 0 5px;">▼</span>	600 <span style="border: 1px solid black; padding: 0 5px;">↕</span>
Web Filter	Access to blocked URL	None <span style="border: 1px solid black; padding: 0 5px;">▼</span>	600 <span style="border: 1px solid black; padding: 0 5px;">↕</span>

Run
Clear
Stop

**Event Logs**

**Welcome!**  
FortiGate Connector is an application providing SDN security for HP environments. As SDN matures and deployment is considered for enterprise networks, the Fortinet and HP SDN integration enables security scenarios between Fortinet's FortiGate Next Generation Firewall and the HP VAN SDN Controller.

Status: clear

Verification: connection to SDN controller was verified

**FortiGate Connector**
HP VAN SDN ▼ Logout

**HP VAN SDN Controller**

IP Address: 10.160.40.32

Username: sdn

Password: ••••••

Domain: sdn

Verify

**FortiGate**

IP Address: 10.160.40.25

Username: admin

Password: •••••

Verify

**Remediation Server**

IP Address:

Discover

Security Type	Event	SDN Action	Timeout(sec)
AntiVirus	Severe virus detected	None <span style="border: 1px solid black; padding: 0 5px;">▼</span>	600 <span style="border: 1px solid black; padding: 0 5px;">↕</span>
Application Control	Detected application to be blocked	None <span style="border: 1px solid black; padding: 0 5px;">▼</span>	600 <span style="border: 1px solid black; padding: 0 5px;">↕</span>
Intrusion Protection	Attack of intrusion detected	None <span style="border: 1px solid black; padding: 0 5px;">▼</span>	600 <span style="border: 1px solid black; padding: 0 5px;">↕</span>
Web Filter	Access to blocked URL	None <span style="border: 1px solid black; padding: 0 5px;">▼</span>	600 <span style="border: 1px solid black; padding: 0 5px;">↕</span>

Run
Clear
Stop

**Event Logs**

**Welcome!**  
FortiGate Connector is an application providing SDN security for HP environments. As SDN matures and deployment is considered for enterprise networks, the Fortinet and HP SDN integration enables security scenarios between Fortinet's FortiGate Next Generation Firewall and the HP VAN SDN Controller.

Status: clear

Verification: connection to FortiGate was verified

FortiGate Connector

HP VAN SDN Logout

**HP VAN SDN Controller**  
IP Address: 10.160.40.32  
Username: sdn  
Password: .....  
Domain: sdn  
Verify

**FortiGate**  
IP Address: 10.160.40.25  
Username: admin  
Password: .....  
Verify

**Remediation Server**  
IP Address: 10.10.10.53  
Discover

Security Type	Event	SDN Action	Timeout(sec)
AntiVirus	Severe virus detected	None	600
Application Control	Detected application to be blocked	None	600
Intrusion Protection	Attack of intrusion detected	None	600
Web Filter	Access to blocked URL	None	600

Run Clear Stop

---

Event Logs

**Welcome!**  
FortiGate Connector is an application providing SDN security for HP environments. As SDN matures and deployment is considered for enterprise networks, the Fortinet and HP SDN integration enables security scenarios between Fortinet's FortiGate Next Generation Firewall and the HP VAN SDN Controller.

Status: clear

Verification: connection to remediation server was verified

## Starting the FortiGate Connector

Once the correct settings have been configured select the **Run** button. The application should start. When the **Status** indicator displays **"running ..."**, it means the FortiGate Connector is ready to receive Syslog information from the FortiGate and to push the flows to the HP VAN SDN Controller.

FortiGate Connector

HP VAN SDN Logout

**HP VAN SDN Controller**  
IP Address: 10.160.40.32  
Username: sdn  
Password: .....  
Domain: sdn  
Verify

**FortiGate**  
IP Address: 10.160.40.25  
Username: admin  
Password: .....  
Verify

**Remediation Server**  
IP Address: 10.10.10.53  
Verify

Security Type	Event	SDN Action	Timeout(sec)
AntiVirus	Severe virus detected	None	0
Application Control	Detected application to be blocked	Prevention	300
Intrusion Protection	Attack of intrusion detected	Remediation	65535
Web Filter	Access to blocked URL	None	600

Run Clear Stop

---

Event Logs

Status: running...

## Stopping the FortiGate Connector

To stop the FortiGate Connector, select the **Stop** button. The **Status** indicator will display "**stopped**". This means FortiGate Connector has stopped all previously pushed flows from being sent to the HP VAN SDN Controller, but the all the configurations are unchanged and maintained.

**FortiGate Connector** HP VAN SDN ▾ Logout

HP VAN SDN Controller		FortiGate		Remediation Server
IP Address:	10.160.40.32	IP Address:	10.160.40.25	IP Address: 10.10.10.53
Username:	sdn	Username:	admin	Verify
Password:	*****	Password:	*****	
Domain:	sdn	Verify		

Security Type	Event	SDN Action	Timeout(sec)
AntiVirus	Severe virus detected	None ▾	0
Application Control	Detected application to be blocked	Prevention ▾	300
Intrusion Protection	Attack of intrusion detected	Remediation ▾	65535
Web Filter	Access to blocked URL	None ▾	600

Run Clear Stop

---

**Event Logs**

**Status: stopped**

## Clear the configuration and stop FortiGate Connector

To clear the FortiGate Controller, select the **Clear** button. The application will stop and configurations will be cleared. When the **Status** indicator displays "**clearing...stopped**", it means the FortiGate Connector has stopped all previously pushed flows from being sent to the HP VAN SDN Controller, and has cleared previous configurations.

**FortiGate Connector** HP VAN SDN Logout

**HP VAN SDN Controller**  
IP Address:   
Username:   
Password:   
Domain:

**FortiGate**  
IP Address:   
Username:   
Password:

**Remediation Server**  
IP Address:

Security Type	Event	SDN Action	Timeout(sec)
AntiVirus	Severe virus detected	<input type="text" value="None"/>	<input type="text" value="600"/>
Application Control	Detected application to be blocked	<input type="text" value="None"/>	<input type="text" value="600"/>
Intrusion Protection	Attack of intrusion detected	<input type="text" value="None"/>	<input type="text" value="600"/>
Web Filter	Access to blocked URL	<input type="text" value="None"/>	<input type="text" value="600"/>

**Event Logs**

**Welcome!**  
FortiGate Connector is an application providing SDN security for HP environments. As SDN matures and deployment is considered for enterprise networks, the Fortinet and HP SDN integration enables security scenarios between Fortinet's FortiGate Next Generation Firewall and the HP VAN SDN Controller.

**Status:** clear

# Supported use scenarios

## Prevention scenarios

- When a user sends a malware file through the network and the FortiGate detects it, the FortiGate Connector will push the flow, along with the user's source IP address and a block action, to the HP SDN controller. The user port of the HP switch will then block all subsequent traffic from this user's IP address.
- When a user generates a botnet command to attack the network that is detected by the FortiGate IPS engine, the FortiGate Connector will push the flow, along with the user's source IP address and a block action, to the HP SDN controller. The user port of the HP switch will then block all subsequent traffic from this user's IP address.
- When a user initiates an application prohibited by the Application Control profile on the FortiGate, the FortiGate Connector will push this application flow, along with the user's source IP address, the destination IP address, the listening port number, and a block action command to the HP SDN controller. The user port of the HP switch then blocks all matching application traffic from this user's IP address. Other traffic from the user is not affected.
- When a user tries to access a web site prohibited by the FortiGate's Web Filter profile, the FortiGate Connector will push this web access flow, along with the user's source IP address, the destination IP address of the web site, and a block action command to the HP SDN controller. The user port of the HP switch then blocks all traffic from the user's IP address to the website's IP address. Traffic from the user to other websites is not affected.

## Remediation scenarios

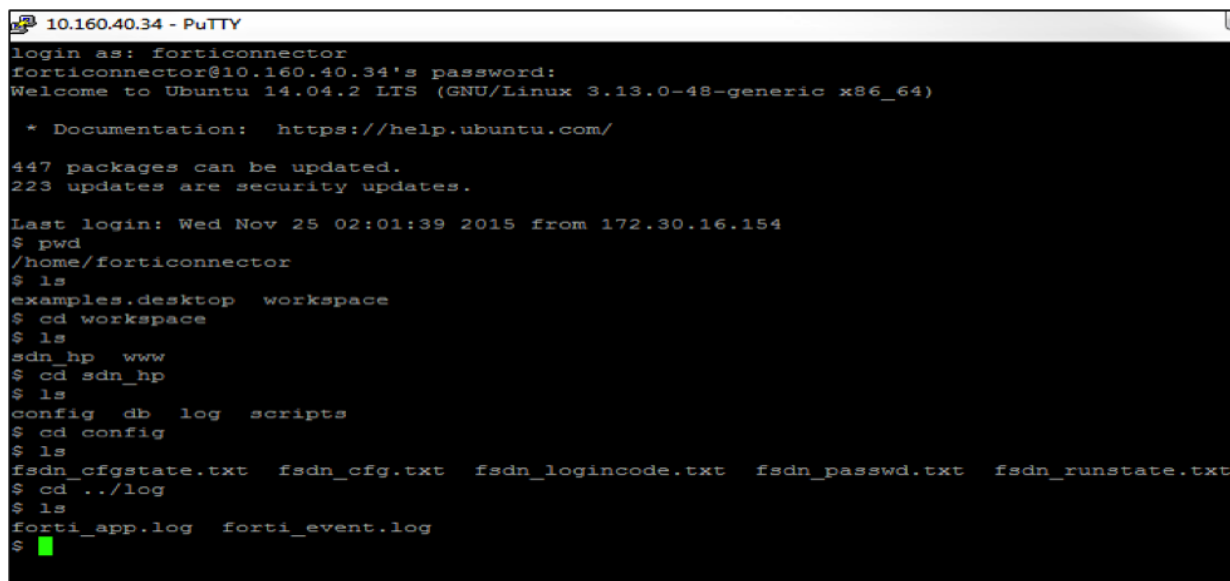
- When a user email containing an attachment of computer virus is sent through the network and detected by the FortiGate, the FortiGate Connector will push the flow, along with user host's source IP address and a redirect action, to the HP SDN controller. The user's subsequent traffic of the source IP will be redirected to the remediation server for corresponding antivirus handling.
- When a user generates a botnet command to attack the network that is detected by the FortiGate IPS engine, the FortiGate Connector will push the flow, along with the user's source IP address and a redirect action, to the HP SDN controller. The user's traffic from the same source IP will be redirected by the HP switch to the remediation server, which enforces a designated policy on the user.
- When a user initiates an application prohibited by the Application Control profile on the FortiGate, the FortiGate Connector will push this application flow, along with the user's source IP address, the destination IP address, the destination port number, and a redirect action command to the HP SDN controller. The HP switch then redirect all matching application traffic from this user's IP address to the remediation server for designated action. Other traffic from the user is not affected.
- When a user tries to access a web site prohibited by the FortiGate's Web Filter profile, the FortiGate Connector will push this web access flow, along with the user's source IP address, the destination IP address of the web site, and a redirect action command to the HP SDN controller. The HP switch then redirect all traffic from the user's IP address to the website's IP address instead to the remediation server for web filtering handling. Traffic from the user to other websites is not affected.



## Basic Troubleshooting

The following are some quick pieces of information that may be helpful in troubleshooting issues that may come up while administering your FortiGate Connector:

- The configuration file is located in the folder: `/home/forticonnector/workspace/sdn_hp/config/`
  - The file is: `fsdn_cfg.txt`.
- Debug messages and event logs are located in the following files:
  - `forti_app.log`
  - `forti_envent.log` (contains events only)
- The syslog messages from the FortiGate are located in the folder: `/var/log/syslog`.



```
10.160.40.34 - PuTTY
login as: forticonnector
forticonnector@10.160.40.34's password:
Welcome to Ubuntu 14.04.2 LTS (GNU/Linux 3.13.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

447 packages can be updated.
223 updates are security updates.

Last login: Wed Nov 25 02:01:39 2015 from 172.30.16.154
$ pwd
/home/forticonnector
$ ls
examples.desktop  workspace
$ cd workspace
$ ls
sdn_hp  www
$ cd sdn_hp
$ ls
config  db  log  scripts
$ cd config
$ ls
fsdn_cfgstate.txt  fsdn_cfg.txt  fsdn_logincode.txt  fsdn_passwd.txt  fsdn_runstate.txt
$ cd ../log
$ ls
forti_app.log  forti_event.log
$
```

### Verify flow pushed by FortiGate Connector on HP SDN Controller for prevention

In order to verify flows pushed by the FortiGate Connector to the HPE VAN SDN Controller, navigate to the flow page on the HPE VAN SDN Controller.

Flows for Data Path ID: 00:01:10:60:4b:b6:2a:40							
Table ID	Priority	Packets	Bytes	Match	Actions/Instructions	Flow Class ID	
n/a	31000	869	55616	eth_type: arp	output: CONTROLLER output: NORMAL	com.hp.sdn.arp.copy	
n/a	60000	0	0	eth_type: bddp	output: CONTROLLER	com.hp.sdn.bddp.steal	
n/a	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 67 udp_dst: 68	output: CONTROLLER output: NORMAL	com.hp.sdn.dhcp.copy	
n/a	31500	246	85116	eth_type: ipv4 ip_proto: udp udp_src: 68 udp_dst: 67	output: CONTROLLER output: NORMAL	com.hp.sdn.dhcp.copy	
n/a	65000	43	0	in_port: 1 eth_type: ipv4 vlan_vid: 3 ipv4_src: 30.30.30.40, mask: 255.255.255.255			Blocked flow from Fortinet Connector
n/a	0	7471	1229593		output: NORMAL	com.hp.sdn.ip.normal	

## Verify flow pushed by FortiGate Connector on HP switch for prevention

In order to verify flows pushed by the FortiGate Connector to the HP Switch

1. Login to the HP switch console.
2. Issue the following command:

HP-Switch# show openflow instance aggregate flows

```

Controller ID : 1                               Cookie : 0xffffc0000babadada
Flow Location : Software
Hardware Index: NA
Reason Code   : 10
Reason Description : The action and output port in the rule is invalid or not supported
Actions
  Controller Port
  Normal

Flow 5
Match
Incoming Port : 1                               Ethernet Type : IP
Source MAC : Any                               Destination MAC : Any
Destination MAC Mask : 0000000-0000000         VLAN Priority : Any
VLAN ID : 3
Source IP Address : 30.30.30.40/32
Destination IP Address : Any
IP Protocol : Any                               IP ToS Bits : Any
Source Port : Any                               Destination Port : Any
Attributes
Priority : 65000                                Duration : 4 seconds
Hard Timeout : 60 seconds                       Idle Timeout : 0 seconds
Byte Count : 0                                  Packet Count : 0
Controller ID : 1                               Cookie : 0x0
Flow Location : Hardware
Hardware Index: 0
Reason Code : 12
Reason Description : Rule is in hardware.
Actions
  Drop ← blocked flow programmed by HP SDN on switch

Flow 6
Match
Incoming Port : Any                               Ethernet Type : Any
Source MAC : Any                               Destination MAC : Any
Destination MAC Mask : 0000000-0000000         VLAN Priority : Any
VLAN ID : Any
Source IP Address : Any                           IP ToS Bits : Any
Destination IP Address : Any                     Destination Port : Any
IP Protocol : Any
Source Port : Any

```

## Verify flow pushed by FortiGate Connector on HP SDN Controller for remediation

In order to verify flows pushed by the FortiGate Connector to the HPE VAN SDN Controller for remediation action, navigate to the flow page on the HPE VAN SDN Controller. The flow matched by the remediation action for redirecting to remediation server can be observed, if the flow was pushed from the FortiGate Connector correctly.

HP VAN SDN Controller

Flows for Data Path ID: 00:01:c4:34:6b:87:fd:00

Table ID	Priority	Packets	Bytes	Match	Actions/Instructions	Flow Class ID
0	0	0	0		goto_table: 100	com.hp.sdn.normal
100	59000	10	0	in_port: 11 eth_type: ipv4 vlan_vid: 3 ipv4_src: 30.30.30.29	goto_table: 200	Matched flow for redirect
100	60000	0	0	eth_type: bddp	apply_actions: output: CONTROLLER	com.hp.sdn.bddp.steal
100	31000	209387	0	eth_type: arp	goto_table: 200	com.hp.sdn.arp.copy
100	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 67 udp_dst: 68	goto_table: 200	com.hp.sdn.dhcp.copy
100	31500	64042	0	eth_type: ipv4 ip_proto: udp udp_src: 68 udp_dst: 67	goto_table: 200	com.hp.sdn.dhcp.copy
100	0	2682089	11134922274...		apply_actions: output: NORMAL	com.hp.sdn.normal
200	59000	11	2016	in_port: 11 eth_type: ipv4 vlan_vid: 3 ipv4_src: 30.30.30.29	apply_actions: set_field: [ipv4_dst: 30.30.30.29] output: NORMAL	Redirected flow from FortiConnector
200	31000	209385	13400640	eth_type: arp	apply_actions: output: CONTROLLER output: NORMAL	com.hp.sdn.arp.copy
200	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 67 udp_dst: 68	apply_actions: output: CONTROLLER output: NORMAL	com.hp.sdn.dhcp.copy
200	31500	64042	22158532	eth_type: ipv4 ip_proto: udp udp_src: 68 udp_dst: 67	apply_actions: output: CONTROLLER output: NORMAL	com.hp.sdn.dhcp.copy
200	0	1626	147869		apply_actions: output: NORMAL	com.hp.sdn.normal

## Verify flow pushed by FortiGate Connector on HP switch for remediation

In order to verify flows pushed by the FortiGate Connector to the HP Switch for remediation action:

1. Login to the HP switch console.
2. Issue the following command:  

```
HP-Switch# show openflow instance aggregate flows
```

```
Flow 8
Match
  Incoming Port : 11
  Source MAC : Any
  Source MAC Mask : 000000-000000
  Destination MAC Mask : 000000-000000
  VLAN ID : 3
  Source IP Address : 30.30.30.29/32
  Destination IP Address : Any
  IP Protocol : Any
  IP ECN : Any
  Source Port : Any
  Source Port Range : NA
  Destination Port Range : NA
  TCP Flags : NA
  TCP Mask : NA
  Ethernet Type : IP
  Destination MAC : Any
  VLAN Priority : Any
  IP DSCP : Any
  Destination Port : Any
Attributes
  Priority : 59000
  Hard Timeout : 60 seconds
  Byte Count : 1084
  Flow Table ID : 200
  Cookie : 0x906cac00
  Hardware Index: NA
  Duration : 5 seconds
  Idle Timeout : 0 seconds
  Packet Count : 4
  Controller ID : 1
Instructions
  Apply Actions
    Modify Destination IP : 30.30.30.29
  Normal
```



**FORTINET®**

*High Performance Network Security*



Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.